CLASS SPECIFICATION
County of Fairfax, Virginia

CLASS CODE: 1833
TITLE: INFORMATION SECURITY ANALYST III
GRADE: S-30

DEFINITION:

Under limited supervision, manages the day to day information protection function and provides supervision to subordinate Information Security Analysts who ensure appropriate security controls are in existence and in force throughout the entire enterprise security architecture; and performs related work as required.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:

This advanced/supervisory information security analysis work is distinguished from the Information Security Analyst II in that the Information Security Analyst III performs work that includes a technical management role with supervisory responsibility and focuses on the entire operational network involving cross-environment security structures, whereas the Security Analyst II performs complex analysis and highly technical tasks involving security measures which focus on a specific or defined security environment.

ILLUSTRATIVE DUTIES:

Performs highly complex analysis and technical tasks involving assignment and coordination of measures to provide information assurance, event detection and rapid response across various environments of the enterprise;
Designs, implements and supports integration of information security solutions including security architectures, firewall administration, integrating security products, and developing and coordinating security implementation plans;
Identifies process functions, risk security weaknesses and controls; presents security challenges and resolutions to management, and implements plans, researches and deploys new technologies, manages transition to operational service
Provides technical lead on security projects which involve a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy;
Provides organizational support of enterprise security architecture and design, benchmarking, technical framework and gap analysis;
Provides organizational support for developing and implementing security of electronic information during transit and on multi-platform operating systems;
Reviews and contributes to the security activities portions of Business Application Development Project Plans;
Works with senior management to determine acceptable levels of risk for enterprise computing platforms and to discuss security implications of new information technology uses being considered;
Reviews and contributes to the improvement and standardization of the security administration process across all business units;

Guides users and technical team members in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and advising alternative approaches;
Interacts with other departments and vendors to gather data, resolve and document complex technical issues for implementation of security products;
Investigates, documents and reports any actual or potential information security violation or inappropriate computers use;
Leads security management services, forensic analysis, cyber-crime investigation, incident emergency response and investigations;
Plans, organizes, coordinates, assigns and evaluates the work of security analysts and technical team members;
Prepares annual budgets and oversees expenditures related to projects;
Manages contracts; directs technical teams to produce deliverables with the project plan timeline and budget;
Prepares training plans for staff, allocates ongoing training for personnel on new computer systems or technologies being implemented which require security administration.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:

Extensive knowledge of data security and access control systems, encryption and related matters;
Extensive knowledge of communications protocols and standards related to security;
Extensive knowledge of information protection methodologies and concepts, such as identification and authentication, access control, inception and audit trails;
Extensive knowledge of server administration as applied to network and internet security;
Knowledge of all areas of technical support for computers, software development, communication systems, networks and their interrelationships;
Knowledge of application systems, network architecture, multiple platforms and new technologies from a security perspective to include the following: Firewalls, Real time Intrusion detection on network and host, Unix, Windows 9X/NT/2000, Novell NetWare, OS390, networking (switches, routers/protocols), TCP/IP, network services and security vulnerabilities, Network Architecture, Token authentication (SecurId), DNS, VPN, Application, Database and O/S Security, as well as web-based systems, Anti-virus, single sign on, PKI, Active directory, and high level programming languages;
Knowledge of system and network exploitation, attack pathologies and intrusion techniques, such as denial of services, Sync attack, malicious code, password cracking, etc.;
Knowledge of information protection standards, guidelines, and applied procedures (i.e. industry “best practices”);
Knowledge of business needs with the ability to establish and maintain a high level of customer trust and confidence in the security team’s concern for customers;
Project management skills;

Ability to perform systems analysis involving identifying and analyzing security controls, performing vulnerability evaluations, conducting risk assessments, developing technical evaluations for various operating systems, authorization methodologies, authentication technologies, monitoring of systems, executing Security Test and Evaluation Plans and Procedures and certification and accreditation;
Ability to formulate conclusions and recommendations and contribute security considerations;
Ability to plan, organize, coordinate, assign and evaluate the work of subordinate staff;
Ability to perform budgeting in support of information security projects;
Ability to interface with individuals at all levels of the organization and to establish effective working relationships;
Ability to communicate effectively, both orally and in writing;
Ability to present and discuss technical information in a way that establishes rapport, persuades others, and gains understanding.

EMPLOYMENT STANDARDS:
Any combination of education, experience, and training equivalent to the following:
Possession of a bachelor's degree in electrical engineering, computer science or telecommunications management; PLUS
Five years of information security systems experience, including supervisory experience.

CERTIFICATES AND LICENSES REQUIRED:
None.

REGRADED: August 23, 2010
ESTABLISHED: August 9, 2001